IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Enrique David Sancho	Examiner: John M. Winter
Application No.:	10/688,734	Group Art Unit: 3685
Filed:	Oct 16, 2003	Docket No.: 2062.001US3
Title:	SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING	
Assignee:	iPass Inc.	

REPLY BRIEF UNDER 37 CFR § 41.41

MS Appeal Brief – Patents
Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

REMARKS

This Reply Brief is filed in response to the Examiner's Answer, mailed April 29, 2011. This Reply Brief supplements the Appeal Brief filed by Appellant on December 13, 2010. Please charge any required additional fees or credit overpayments to Deposit Account 50-3998. The Appellant has reviewed the Examiner's Answer and believes the statements in the Appeal Brief remain accurate and compelling. In responding to the Examiner's Answer, Appellant provides the following discussion.

Claims 34-36, 40 and 43-44 are improperly rejected under 35 U.S.C. §103 as being unpatentable over Pare Jr. et al. (US Patent 6,269,348) in view of Glass et al. (US Patent 6,332,193).

In the Response to Argument, the Examiner indicated the following:

> In regard to claim 34, the Appellant states Pare Jr. et al. does not teach a first server receiving a computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer.

> The Examiner responds that Pare Jr. et al. discloses an identification module comprising biometric data and Pin as well as a hardware identification code (Column 11, lines 15-21), The Examiner submits that because the hardware identification code uniquely identifies the users computer it teaches the claimed feature of "computer fingerprint file. The Appellant states that Pare's passage does not teach the first server's comparing operation.
>
> The Examiner responds that Pare Jr. et al. discloses receiving biometric sample which includes a hardware identifier for identification and utilizing a database to determine if a stored value matched the received value (Column 11, lines 39-48) the Examiner submits that this teaches the claimed feature of " identifying the user computer based on information associated with a plurality of components included in the user computer; comparing the first computer fingerprint file against a second computer fingerprint file to verify the user computer"[1]

Appellant respectfully traverses. These sections of Pare do not disclose this element of claim 34. In particular, Pare at column 11, lines 15-21 and 39-48 disclose operations wherein the hardware code is used to identify a party (the payee) (not to identify a user computer):

> In a preferred embodiment, identification module 30 comprises subsystems that can **identify parties** from the following information:
>
> biometric data and PIN
> biometric data alone
> digital identification (digital certificates)
> **PIA hardware identification code**
> Biometric-PIN Identification Subsystem (BPID)[2]
>
> Once a BPID processor receives a bid biometric sample and PIN for identification, the processor searches through its database, retrieving all registered biometric samples that match or correspond to that particular bid PIN. Once all corresponding registered biometric samples are retrieved, the processor compares the bid biometric from the message to all retrieved registered biometric samples. If a match is found, the processor transmits the **identity of the party** back to TP 26. If no match is found, the processor transmits a "**party not identified**" message back to TP 26.[3]

[1] Examiner's Answer at pages 6-7.
[2] Pare at col. 11, lines 15-21.
[3] Pare at col. 11, lines 39-47.

Also, in the Response to Argument, the Examiner indicated the following with regard to the operations at the second server:

> The Appellant states that Glass does not teach receiving a second identification message at a second server.
>
> The Examiner submits that Glass discloses, a system that returns a previously generated token from a client to a server for authentication (Column 10, lines 30-38), since this token was previously generated the Examiner submits that the return of the token constitutes a "second message at a second server". Furthermore the Examiner submits that claimed limitation regarding a second server are merely a duplication of a claim element and as such do not have patentable merit. Mere duplication of parts has no patentable significance unless new and unexpected result is produced. In re Harza, 124 USPQ 378 (CCPA 1960).[4]

Appellant respectfully traverses. First, the claimed limitations performed at the second server are not duplications of any other limitation. Therefore, such limitations have patentable weight. In particular, the operation performed at the first server includes comparing a first computer fingerprint file to a second computer fingerprint file. In contrast and not duplicative of the operation at the first server, the operation performed at the second server includes comparing a first identification for a user to a second identification for the user. Accordingly, the operations performed at the second server have patentable weight with regard to claim 34.

Also, Appellant respectfully submits that Glass does not disclose the operations performed at the second server:

> receiving, at a second server, a second message from the user computer, the second message including a first identification for the user, the first identification being associated with the first computer fingerprint file identifying the user computer; and
>
> comparing, at the second server, the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second mini-server; and

[4] Examiner's Answer at pages 7-8.

> after the comparing of the first identification for the user against the second identification for the user to verify the user, generating a third message, at the second server, based upon the results of the comparison.

In particular, the cited section of Glass (col. 10, lines 30-58) does not disclose the operations performed at the second server. This section of Glass describes a computer sending an image to a server, where the image was captured by a camera connected to the computer. Along with the image, the computer sends a digital signature and camera's unique serial number to the server. The digital signature and serial number are either embedded directly into the image or alongside the image in a data packet. The server sends the serial number to a central camera certification authority which looks-up the camera's public key and returns the public key to the server. Using a token (generated earlier) and the camera's public key, the server re-calculates the digital signature to ensure the image has not been tampered with. Appellant submits that Glass' complex image authentication process does not teach or suggest claim 34's operations for verifying user identification information.

Accordingly, Applicant respectfully submits that claims 34 and 40 are patentable over the cited references. Because claims 35-36 and 43-44 depend from and further define claim 34, Applicant respectfully submits that claims 35-36 and 43-44 are patentable over the cited references.

CONCLUSION

It is respectfully submitted that the claimed invention is patentable in view of the cited art. It is respectfully submitted that claims 34-36, 40, and 43-44 should therefore be allowed. Reversal of the Examiner's rejections of claims 34-36, 40, and 43-44 is respectfully requested.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-3998.

Respectfully submitted,

DeLizio Gilliam, PLLC
15201 Mason Road
Suite 1000-312
Cypress, TX 77433
281-758-0025

Date 6/29/2011 By /Gregg A. Peacock #45001/
Gregg A. Peacock
Reg. No. 45,001

This paper or fee is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.